ByBox

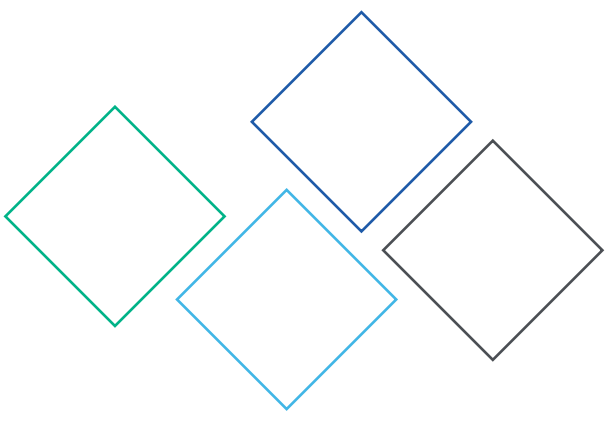
KEEP YOUR WORLD WORKING

Third Party Data Protection Policy

VERSION 3
Date: 22nd of May 2018
Document owner: ByBox Information Security Management Group

www.bybox.com

Contents



INTRODUCTION

ByBox is entirely committed to complying with Data Protection Legislation, in order to protect the personal privacy of all individuals whose data we hold. ByBox group companies are registered, with the Information Commissioner's Office, as Data Controllers (our registration number is: Z815832X). This policy outlines how ByBox will comply with Data Protection obligations when handling personal data relating to ByBox customers and other third parties.

When we handle personal data under contract with our business customers and other third parties (e.g. users' delivery details that are passed to us by business customers), as a processor, we have specific legal obligations to protect that data. ByBox is committed to ensuring all personal data relating to its customers and other third parties is handled securely and with proper regard for their privacy. Compliance with this policy will help ensure that all personal data held by ByBox is handled lawfully.

All ByBox staff are required to comply with this Policy. Compliance with this policy is a condition of employment and any deliberate breach of this policy will result in disciplinary action, which may include dismissal and possible prosecution.

DATA PROTECTION PRINCIPLES

Data Protection Legislation governs the handling of personal data. Personal data is information in any format which relates to an identifiable living individual.

ByBox will comply with data protection law. This says that the personal information we hold about an individual must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected only for specified, explicit and legitimate purposes.
- Processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Accurate and kept up to date with all reasonable steps taken to ensure that inaccurate personal data is rectified or deleted without delay.
- Kept only for the period necessary for processing.
- Secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

In order to comply with these principles ByBox will:

- ensure personal data is used fairly and only in accordance with the expectations of affected individuals

- meet its legal obligations to specify the purposes for which personal data will be used, by including relevant information within its on-line privacy policy and on the face of any paper-based data collection forms.
- collect and process personal information only to the extent necessary for operational purposes or to comply with legal requirements.
- take reasonable steps to ensure that personal data is accurate and up to date.
- retain personal data only for so long as this is necessary having regard to legitimate operational need and the expectations of individuals concerned.
- ensure that individual data subject whose data is held by ByBox are able to exercise their rights, particularly their rights to request copies of their personal data
- take appropriate technical and organisational security measures to safeguard personal information.
- ensure that any contractors engaged to handle personal data on our behalf are properly supervised and are subject to appropriate contractual controls
- provide all staff who are involved in handling personal data with appropriate and relevant training
- ensure that personal information is not transferred to a country outside Europe without suitable safeguards.
- audit data security and compliance with this policy on a periodic basis.

PURPOSES FOR WHICH PERSONAL DATA ARE HELD

Data relating to individual users of ByBox services is held by ByBox for the purpose of:

- service delivery,
- invoicing,
- product and business development.

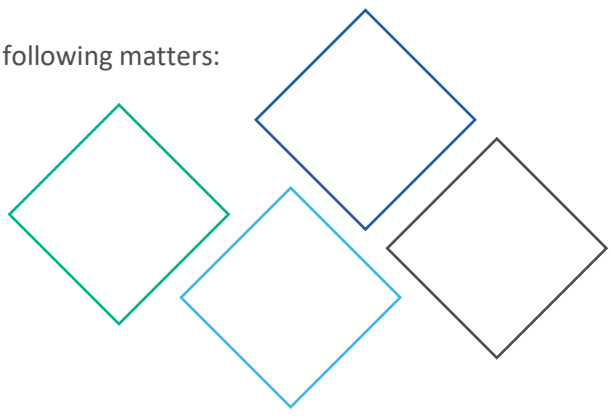
ByBox will not use its customer data for other unrelated purposes without consent unless required to do so by law.

SENSITIVE PERSONAL DATA

Sensitive personal data includes information relating to the following matters:

Information as to a person's

- racial or ethnic origin.



- political opinions.
- religious or similar beliefs.
- trade union membership.
- physical or mental health or condition.
- sexual life.
- The commission or alleged commission of any offence
- The outcome of any prosecution

ByBox does not normally hold sensitive personal data relating to customers or other third parties. However, personal data falling within these categories is subject to additional protection and, therefore, where sensitive data is collected for any reason, we endeavour to obtain consent from the individuals concerned.

USE OF PERSONAL DATA

When a customer tries, purchases, uses, subscribes or obtains support for our products, ByBox collects data to provide its services, operate its business and communicate with the customer.

PRE- SALES PROCESS

When a customer engages with a sales representative, ByBox collects the customer's name and contact data, along with information about the customer's organisation, to support that engagement. For logistics services, ByBox may also obtain the home postcodes of engineers, this is to carry out a mapping exercise to identify and allocate the appropriate ByBox lockers.

IN DELIVERING OUR CORE SERVICES

In delivering our services the types of personal data we process may include:

For users and administrators:

(1) business contact names, business phone numbers, business addresses,

For users:

(2) user home addresses (for mapping purposes).

.

For certain users the type of data may also include:

(3) user location tracking data,

To provide location-based services on ByBox products, location data functionality may be enabled on users' devices but only for the purposes of notifying of the location of the nearest ByBox locker; this functionality may be disabled (by the user) at any time. The location data does not leave a user's device and is not stored on our database.

IN DELIVERING OUR CUSTOMER SUPPORT SERVICES

To support our customers and provide an excellent service to our customers our Account Management Team store names, phone numbers, email addresses and engineer addresses

When a customer interacts with a ByBox customer support professional, we collect data to diagnose and resolve problems.

RESPONSIBILITY FOR THE PROCESSING OF PERSONAL DATA

Mark Bromwell (CTO) is ultimately responsible for the processing by ByBox of personal data.

All employees who have access to personal data are responsible for complying with this policy and with other relevant policies and procedures relating to data handling. Failure to comply with these policies and procedures may result in disciplinary action up to and including summary dismissal.

DATA QUALITY

ByBox is required to ensure that personal data that we process is

- relevant, adequate and not excessive
- accurate and up to date
- not held for longer than is necessary

Complying with these obligations makes good business sense and is important to protect individual privacy. ByBox will therefore review periodically the customer data it collects in order to ensure that this data is adequate and relevant to the services we provide and is not excessive. We will also make it easy for our customers to let us know of any change in their circumstances so that we can update

our records accordingly. All information will be disposed of securely when no longer required in accordance with our Retention Policies and our Secure Disposal Policy.

RETENTION POLICIES:

Pre-Sales communications

In the event that we are in touch with you marketing our services, but no supplier relationship develops, our policy is to retain any personal data for up to 3 months following the last communication.

Customer/ other third party personal data

Our standard policy is to retain personal data for up to 3 months following the termination of associated services– we retain the data for this 3 month period in order to facilitate addressing/investigating any queries that our customers may have relating to associated services supplied.

Location tracking data

We do not collect and/or retain location tracking data.

DATA SECURITY

Information Security is a matter of priority for ByBox as our customers rely on us to look after their personal information.

Data security includes IT and physical security but also refers to the systems, policies and procedures that are necessary in order to guard against loss, damage, destruction of personal data and against inappropriate or unlawful access. ByBox is ISO 27001 accredited.

Data security depends very considerably on staff training and awareness. ByBox is committed to ensuring that all staff with data handling responsibilities receives appropriate training in relation to data security and confidentiality. In addition, our policy detailing Employee Data Protection Obligations can be found here:

ByBox recognises that the use of external contractors to handle personal data usually creates additional data security risks. ByBox acknowledges that a specific requirement of Data Protection Legislation, is that any contractors that are engaged to handle personal data on our behalf, must be carefully selected and properly supervised. Therefore, whenever a contractor is engaged to carry out work that involves the processing of personal data, ByBox will allow the contactor to handle personal data only if we are satisfied that the contractor's data security measures are adequate and

only where a written contract setting out the contractor's obligations in relation to that data are clearly set out in accordance with Data Protection Legislation.

DATA SECURITY BREACHES

Any data security breach should be reported to the ByBox CTO so that action can be taken to protect affected individuals and to ensure that lessons are learned to minimise the risk of recurrence.

If ByBox discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. ByBox will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

ONWARD DISCLOSURE OF PERSONAL DATA

We share your personal data with the relevant personnel within ByBox to operate our services effectively. We may also share your personal data with our corporate group which means our subsidiaries, our ultimate holding company and its subsidiaries; with subcontractors working on our behalf; when required by law or to respond to legal process; to protect our customers; to protect lives; to maintain the security of our products; and to protect the rights or property of ByBox.

We may disclose your personal information to third parties:

- In the event that we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets.
- If we, or substantially all of our assets, are acquired by a third party, in which case personal data held by us about our customers will be one of the transferred assets.
- In order to enforce or apply contractual terms, to investigate potential breaches or to protect the rights, property or safety of our customers and others (this may include exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction).
- Where this is required by law or where this is necessary for the performance of a service we provide to you.

In exceptional circumstances the legislation does permit personal data to be disclosed to third parties without consent. Examples include disclosures to statutory bodies for the purpose of detecting crime, fraud or money laundering or disclosures necessary for medical purposes.

If, exceptionally, it is necessary to disclose personal data to third parties, ByBox will ensure that this is done securely and in a manner that minimises privacy risks.

INDIVIDUAL'S RIGHTS

Any individual can exercise its rights against us in relation to the information we hold about them.

Individuals have a number of other rights in relation to their personal data. They can require us to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the ByBox's legitimate grounds for processing data (where ByBox relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override ByBox's legitimate grounds for processing data.

To ask ByBox to take any of these steps, the individual should send the request to HR@bybox.com.

To read more about these rights click here - https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/.

ACCESS TO PERSONAL DATA ("SUBJECT ACCESS REQUESTS")

Individuals have the legal right to request the disclosure of personal data relating to them that is held by ByBox. ByBox must provide a copy of the information free of charge, however we can charge a reasonable fee when a request is manifestly unfounded, or excessive.

Anyone seeking to make a subject access request should be asked to supply evidence of their identity and make their request in writing. Where a subject access request is submitted to us, a full response should be issued within one month. There are some exemptions from the duty to supply information, especially where disclosure will involve the disclosure of information about other people. If there are any concerns about the disclosure of information in response to a request, advice should be sought.

REQUESTING DATA

On completion of the form below. Please forward to the following e-mail address HR@bybox.com. Your request will be actioned accordingly, and you will be kept informed as to how your request is progressing.

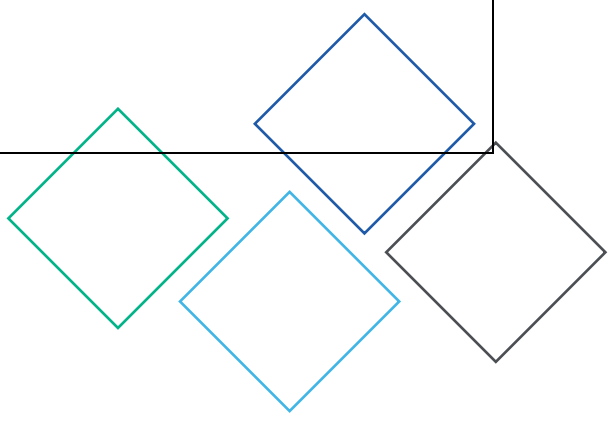
Subject Access Request

Applicant Details	
Name of Applicant:	
Address of Applicant:	
Email address:	
Telephone:	

Where Applicable	
Company Name:	
Department Name:	

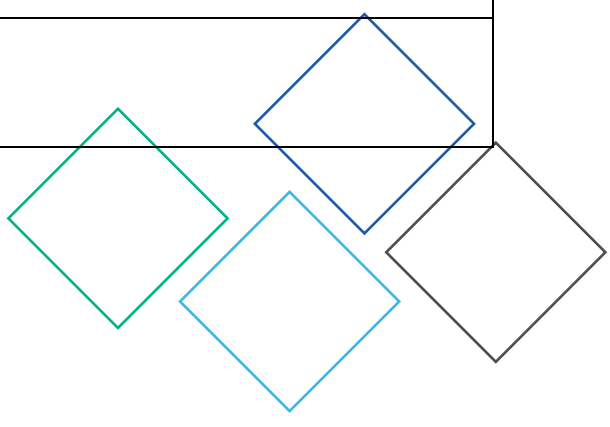
Company Address:	

Nature of Enquiry		
Reason for Request	Without it, the prevention or detection of crime will be prejudiced	Yes / No
	Without it, the apprehension or prosecution of offenders will be prejudiced	Yes / No
	Other, please specify:	
Location:		
Date and Time:		
Subject Name (if applicable):		
Required Information:		



Please complete this section if information is being requested by a company on behalf of a third party data subject

Authorisation (to be completed by an authorised person)	
Name:	
Title:	
Date:	
Signature:	



Email address:	
Telephone: